****

**Digital forensics in law enforcement practical exercise**

This document contains instructions and tasks for a digital forensics’ lab. The lab begins with factual questions which offer an opportunity to explore Autopsy Forensics and forensic examinations. The second part of the lab includes a small criminal case where the task is to use Autopsy Forensics to find evidence related to that case. The disk image for the lab is called phishy.E01. The disk image is provided by the course teacher.

Suggested reading for this lab is:

* CyBOK knowledge area Forensics
* https://link.springer.com/content/pdf/10.1007/978-3-030-38954-3.pdf

The lab and disk image are developed by Joakim Kävrestad and Jönköping School of Engineering. For issues and questions, contact Joakim at Joakim.kavrestad@ju.se

**Note that the lab was created using Autopsy version 4.21.0**

© Crown Copyright, The National Cyber Security Centre 2024. This information is licensed under the Open Government Licence v3.0. To view this licence, visit <https://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/>.

When you use this information under the Open Government Licence, you should include the following attribution: CyBOK memory analysis workshop slides © Crown Copyright, The National Cyber Security Centre 2024, licensed under the Open Government Licence: <https://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/>.

**Lab step 1.**

The first part of the lab is designed to allow students to explore Autopsy forensics and use it to find fundamental artifacts. To begin, create a new case in Autopsy and load the forensic disk image Phishy.E01. Make sure that you do NOT run any ingest modules at this stage. To import Phishy.E01, ensure that you unzipped phishy.zip and now have a folder with the filed Phishy.E01, Phishy.E02, …, Phishy.E11. All those files are part of the image, but you only need to direct autopsy to the one ending with E01. If they are all in the same folder, Autopsy will know how to piece them together. When the image is loaded, answer the following questions. As a rule, provide your answer and a short description of how you found it.

1. What is the total size of the disk in bytes and sectors?
2. How many partitions are there?
3. What is the total number of sectors NOT allocated to any partition?
4. What is the starting sector of the partition where the operating system is installed?
5. How many user home folders are present on the partition identified in Q4?
6. How many folders are there in the “Program Files” folder?
7. How many folders are there in the “Program data” folder?
8. How many image files does the image contain?
9. How many deleted files are contained in the image?
10. What is the name of the largest video file?

Now run the ingest modules *File Type Identification and Extension Mismatch Identification.* Depending on your computing power, this may take some time.

1. How many JPEG images are identified by Autopsy?
2. How many files are flagged as “extensions mismatches”?

Now run the ingest module “Encryption detection” with default options.

1. How many files are flagged as possibly encrypted?

Now run the ingest module “Recent Activity”.

1. What was the name of the last accessed file?
2. What is the username of the active computer user?
3. What operating system was the computer using?

Now run the ingest module “Picture Analyzer”.

1. What device was used to take “hidden3.jgp”?
2. What are the GPD coordinates of “IMG\_1485.jpg"?

**Lab step 2.**

The second part of the lab is for you to conduct a forensic examination in a crime setting. You are expected to look for evidence of interest for a criminal investigation relating to fraud. More specifically, the disk image is from the computer of someone suspected of crafting phishing emails and sending those to specific victims. The following three questions should guide your analysis:

* Has the computer user been sending phishing emails?
* Who are possible targets of those emails?

Use autopsy to find evidence that may be of interest for this case. Report your findings in a forensic protocol. When writing your forensic protocol, remember that it should be tangible for non-technical readers, be objective, and clearly separate facts from your conclusions.